Jali Rintakorpi

TIETOTURVASUUNNITELMA MIKROYRITYKSELLE

Tietojenkäsittelyn koulutusohjelma

2017

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

TIETOTURVASUUNNITELMA MIKROYRITYKSELLE

Rintakorpi, Jali
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Lokakuu 2017
Ohjaaja: Nuutinen, Petri
Sivumäärä: 38
Liitteitä: 0

Asiasanat: tietoturva, tietosuoja, tietoliikenneverkot, suunnitelmat, mikroyritykset

---

Tämän työn tarkoitus on tutkia mikroyritysten mahdollisia puutteita ja tuoda käytettävää hyötyä tietoturvan parantamiseksi. Tässä työssä ei yritetty saavuttaa täydellisyyttä, vaan sen on tarkoitus toimia pohjana pienemmille yrityksille. Työssä tutkittiin mielikuvituksellisen alle 10 työntekijän mikroyrityksen tietoturvaa. Yrityksen tietoturvatarpeet keksittiin käyttämällä paikallisen yrityksen osittaisia tietoja pohjana, jonka päälle rakennettiin ongelmia. Parannusehdotukset tehtiin työssä määritellyn yrityksen ongelmien mukaan.

Fyysistä tietoturvaa käsiteltiin enemmän laitteiden suojaamisen ja huoltamisen kannalta. Fyysisten riskien ehkäisyä pyrittiin myös huomioimaan. Vesivahingot ja sähkökatkokset nähtiin mahdollisina infrastruktuurin riskitekijöinä tietoturvan kannalta. Ihmisten tekemät virheet ja mahdolliset varkaudet nähtiin myös mahdollisina riskitekijöinä.

Digitaalisen tietoturvan osalta yrityksen yhteyksien turvaaminen oli tärkeä osa tätä työtä. Yhteyksiä turvattiin hankkimalla oikeat ja tarvittavat laitteet. Hyväksi ratkaisuksi tähän tehtävään määriteltiin olevan uuden palomuurilaitteen hankkiminen vanhan modeemin/reitittimen jatkeeksi. Kunnollisten varmuuskopioiden puute nähtiin myös suurena riskitekijänä tietoturvan jatkuvuuden osalta. Tätä korjattiin hankkimalla tarvittavat laitteet kahta uutta varmuuskopiota varten. Yritykselle luotiin myös salasanapolitiikka, jota yrityksessä ei ennen ollut.

Tietoturvaa käsiteltiin suhteellisen laajasti ja työssä käsiteltiin mikroyrityksille sopivasti liittyviä asioita. Tässä työssä ei tutkittu mikroyritykselle liian monimutkaisia ratkaisuja. Työssä yritettiin pysyä tärkeissä ja loogisissa tietoturvaa parantavissa vaihtoehdoissa. Hintaa yritettiin myös ottaa osaksi yrityksessä tehtäviin muutoksiin.

SECURITY PLAN FOR MICRO COMPANY

Rintakorpi, Jali
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Data Processing
October 2017
Supervisor: Nuutinen, Petri
Number of pages: 38
Appendices: 0

Keywords: data security, data protection, telecommunication networks, plans, micro companies

---

The purpose of this work was to study possible information security shortcomings in micro enterprises and give usable advice to improve their security. This work does not try to achieve perfection, but it's supposed to act as a basis for smaller companies. In this work, I studied information security of an imaginary micro enterprise with less than 10 employees. The company and all its problems were thought up by using a local micro enterprises information as a basis. All the improvement recommendations to information security were based on the imaginary enterprise's needs.

Physical information security was dealt with more in the protection and maintenance of equipment. Physical risk prevention was also considered. Water damages and electric outages were considered as potential infrastructure risk factors to information security. Errors made by employees and possible thefts were also under consideration.

Creating secure connections were an important part of information security in this work. Connections were secured by getting proper and necessary equipment. New firewall device was a good solution to complement the company's old modem/router. The lack of proper backups was also a major risk factor for data continuity. This was fixed by getting two new devices for backups. Password policies also did not exist so they were created.

Information security was studied quite broadly and everything was thought out by keeping micro enterprises needs in mind. This work does not study complicated solutions for a micro enterprise and study was based more on important and logical solutions for information security for a micro enterprise. Price was also partially taken into consideration as part of implementation of this plan for the company.

SISÄLLYS

1 JOHDANTO

Tietoturva on tärkeää kaikissa yrityksissä, mutta pienemmät yritykset saattavat olla sen osalta skeptisiä ennen kuin jotain pahaa on jo sattunut. Tietoturvasta huolehtiminen on kuitenkin aina tärkeää, kun yrityksessä käytetään mitä vain laitteita, jotka taltioivat suojassa pidettäviä tietoja. Näitä tietoja ovat esimerkiksi asiakastiedot, sopimukset ja yritykseen liittyvät dokumentit. Kaikki tieto on silti hyvä turvata, vaikka tieto ei olisikaan niin tärkeää tai salassa pidettävää. Tietoturvan tarkoitus on myös varautua tietovarkauksiin, hakkerointiin, haittaohjelmiin ja muihin mahdollisiin vaaratekijöihin.

Tietoturvasuunnitelman tulisi sisältää käytännöllinen suunnitelma riskeihin valmistautumista varten. Suunnitelmassa tulisi käsitellä riskien tunnistamista ja niiden ehkäisyä. Kaikkeen ei voida tietenkään aina varautua, mutta suunnitelman tekeminen helpottaa riskien hallintaa. Työntekijät aktivoidaan paremmin mukaan tietoturvan huolehtimiseen kouluttamalla heitä ja määrittämällä heidän tietoturvavaatimuksensa. Tietoturvasuunnitelman kuuluisi myös määritellä kenellä on oikeus käyttää mitäkin resursseja tarvittaessa. (Yeagley, 2015.)

2 TIETOTURVASUUNNITELMAN TÄRKEYS

Tietoturvasuunnitelman tarkoitus on pitää yrityksen tieto suojattuna. Suunnitelman avulla saadaan määriteltyä tarvittavat suojaustoimenpiteet ja tavat, joilla tietoja tulee suojata ja käsitellä. Kolme tärkeintä asiaa, jotka määritellään tietoturvasuunnitelmalla, ovat luottamuksellisuus, tiedon eheys ja tiedon saatavuus. Luottamuksellisuudella määritellään kenelle tietoa saa tai ei saa jakaa. Tiedon eheydellä määritellään tiedon säilyvyys niin, että se on oikeaa ja se on turvattu ulkopuolisia uhkia vastaan. Tiedon saatavuudella määritellään, miten tietoa käsitellään sekä taataan, että tieto on yrityksen käytettävissä aina tarvittaessa. (Krzyzweski, 2.)

Yrityksen koolla ei ole väliä vaan jokaisella yrityksellä tulisi olla tietoturvasuunnitelma. Suunnitelman pituudella ei ole niin väliä, kunhan suunnitelma on yritykselle ja sen tarpeille suunniteltu. Se auttaa yritystä ajattelemaan toimintaansa turvallisemmin ja välillä päivittämällä tietoturvasuunnitelmaa saadaan yrityksen turvallisuus pidettyä ajan tasalla. (AppliedTrust www-sivut.)

Nykyaikana yrityksen arvo voidaan mitata sen tiedon mukaan ja jos tietoa ei suojella tarpeeksi hyvin saattaa yrityksen arvo romahtaa täysin, jos se kaikki menetetään. Tietoturvasuunnitelmaa tehdessä kannattaa arvioida tietojen tärkeyttä yritykselle. Esimerkiksi asiakastietojen menetys on yleensä todella iso takaisku, joten niitä varsinkin kannattaa suojata hyvin. Muina esimerkkeinä tärkeitä tietoja voivat olla yrityksen suunnitelmat, patentit, piirustukset ja tietenkin yrityksen taloudelliset tiedot. (AppliedTrust www-sivut.)

3 UHAT

3.1 Fyysiset uhat

Fyysisiä uhkia tietokoneille on monia. Uhat voivat olla pieniä asioita, joista syntyy isoja ongelmia. Digitaaliset tallenteet ovat uhattuina ulkoisista kuin myös sisäisistä voimista. (Digital Preservation Management www sivut.)

Fyysisiin uhkiin kuuluu seuraavat asiat (Digital Preservation Management www sivut):

- Vääränlaiset säilytys olosuhteet (lämpötila, ilmankosteus, pöly)
- Fyysisten osien liiallinen käyttö
- Laiteviat
- Vähäinen laitteiden huolto
- Luonnon uhat (tulipalo, tulva)
- Infrastruktuurin viat (vesiputket, sähkölinjat)
- Ihmisten tekemät virheet

- Sabotaasi (varkaus, ilkivalta).

3.1.1 Säilytysolosuhteet

Tietokoneet ovat herkkiä elektronisia laitteita. Niitä kannattaa siis säilyttää hyvissä olosuhteissa ongelmien välttämiseksi ja laitteiden pitkän iän saavuttamiseksi. Tietokoneita sisältävien huoneiden ei saa antaa kuumentua liikaa kuin myös niiden ei saisi antaa viilentyä liikaa. Tietokoneita ja muita laitteita sisältävät huoneet tulisi pitää 18°C ja 27°C välillä. (AVTECH www sivut.)

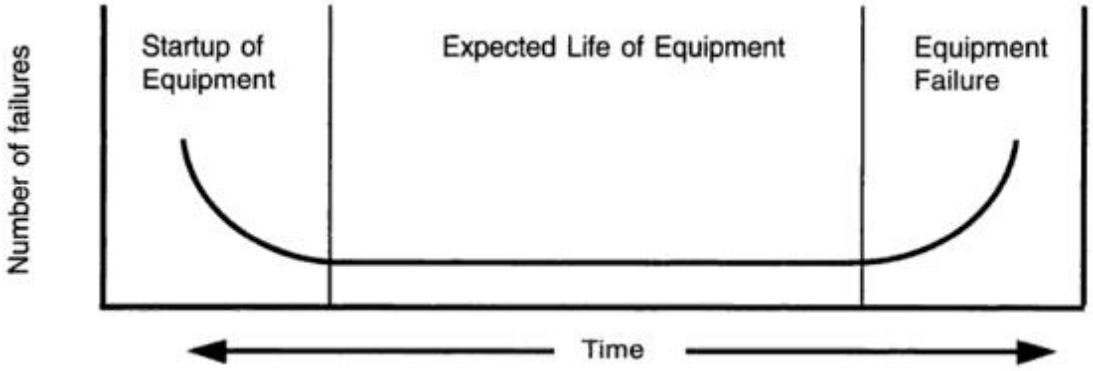
Ilmankosteus on myös tärkeä pitää hyvässä tasossa tietokoneita sisältävissä huoneissa. Suositeltu ilmankosteus on noin 40% ja 60% välillä. Matalin taso johon ilmankosteuden saisi päästää on 20% ja korkein mihin se saisi nousta on 80%. Liian matala ilmankosteus aiheuttaa sähköstaattisia purkauksia, jotka vahingoittavat laitteita. Korkeat ilmankosteudet taas aiheuttavat kondensaatiota, joka aiheuttaa korroosiota laitteissa ja rikkoo laitteita. (AVTECH www sivut.)

3.1.2 Fyysisten osien liiallinen käyttö, laiteviat ja huoltaminen

Laitevikoja tulee vastaan joka yrityksessä ja niihin ei aina haluta varautua tarpeeksi hyvin. Huoltamiseen kuluu rahaa ja ihmisten työaikaa sekä asiakkaat kärsivät, jos palvelin on sammutettuna pitkiä aikoja. (Rood 1996, 3.) Tietokoneita tulisi kuitenkin päivittää noin 3 – 5 vuoden, koska sen jälkeen laitteiston huoltokulut alkavat olla korkeat. Yli 5 vuotta vanhojen laitteiden huoltokulut voivat olla jopa 200% alkuperäistä suuremmat, kun taas yli 7 vuotta vanhoilla laitteilla se voi olla jopa 400%. Järjestelmät kannattaa uusia mieluummin silloin kun ne toimivat sen sijaan kuin alkaa korvata rikkinäisiä laitteita. (Nordquist 2017.)

Laitteiden fyysinen rasitus ja niiden oikeanlainen huoltaminen ovat myös tärkeä osa tietoturvallisuutta. Yllättäviä laiterikkoja ei halua ketään, koska niistä voi koitua tietojen menetystä. Laitteiden huoltotarpeet ovat yleensä suurimmat uuden laitteen hankinnan yhteydessä, sekä niiden elinkaaren loppupäässä (kuva 3). Laitteet kannattaa

siis huoltaa tai korvata tietyin aikavälein mielellään jo hieman ennen kuin ne pettävät lopullisesti. (Rood 1996, 4)



Kuva 3. Laitteiden odotettu elinkaari ja niiden viat (Rood 1996, 4).

Tietokoneita tulisi huoltaa pitämällä ne puhtaina ja puhaltamalla niiden sisältä pölyt pois usein. Pöytätietokoneet varsinkin keräävät paljon pölyä sisäänsä ja aiheuttavat ylikuumentumista, joka taas vähentää osien elinikää. Laitteet tulisi puhdistaa vähintään kerran vuodessa, mutta mielellään jopa 2–3 kuukauden välein. Hyviä välineitä puhdistuksessa ovat paineilmapurkki ja mikrokuituliinat. (Steers 2004.)

3.1.3 Luonnonuhat ja infrastruktuurin viat

Tulipalot ovat vaikea asia hallita toimistotiloissa oleville laitteille. Vesisammutusjärjestelmät ovat laitteille haitallisia ja kaasupohjaiset sammutusjärjestelmät ovat vaarallisia ihmisille. Vesisammutusjärjestelmää käytettäessä tulisi päävirta saada katkaistua nopeasti, jotta laitteissa ei kulkisi sähköä. Virran katkaisu minimoi riskiä laitteistolle. (Wallace 2017.)

Tulvat ja vesivahingot myös ovat yksi uhka järjestelmille, varsinkin jos niihin ei ole valmistauduttu kunnolla. Laitteet tulisi säilyttää paikassa, jossa ei mene vesiputkia seinissä eikä katossa. Niiden pitäisi olla myös tarpeeksi korkealla, etteivät ainakaan vähäiset tulvat tai lattialle valuva vesi pääse niitä vahingoittamaan. Tarvittaessa laitteita voi myös suojata ”sateenvarjoilla”, ettei vaikka katosta läpi vuotava vesi pääse niihin. (Wallace C, 2017.) Porin alueella varsinkin tulvat ovat todellinen riski. Tulvia

on historiassa tapahtunut noin 10–20 vuoden välein ja vesistötulvista johtuva vahingonvaaran riski on Suomen suurin. (Porin kaupungin www sivut.)

3.1.4 Ihmisten virheet ja varkaudet

Työntekijät ovat aina riski yrityksen tietojen menetykselle. Suuri osa yrityksen tietoturvamurroista johtuu yleensä työntekijöiden virheistä ja heidän vahingossa vuotamistaan tiedoista. Työntekijät saattavat käyttää helposti arvattavia salasanoja ja käyttäjätunnuksia, he voivat kadottaa laitteita, lähettää tietoa vääriin sähköpostiosoitteisiin, selata vaarallisia sivuja, jakaa salasanojaan muille, jättää tietokone auki lähtiessään sen ääreltä pois ja he voivat käyttää suojaamattomia yksityisiä laitteita yrityksen verkossa. (Deursen, N. 2015.)

3.2 Digitaaliset uhat

Tietojärjestelmät ovat usein avoinna monille erilaisille uhille. Erilaisista uhista aiheutuvat vahingot voivat aiheuttaa niin pieniä kuin myös suuria rahallisia menetyksiä yrityksille. Digitaaliset uhat voivat olla tiedon menetykseen johtavia tai järjestelmien toimintaan vaikuttavia tekijöitä (Procedia Computer Science, 1). Teknologian kehityksen jatkuessa uusia uhkia ilmenee jatkuvasti ja niitä ei voida kaikkia aina tunnistaa nopeasti (Procedia Computer Science, 2).

Digitaalisten uhkien lähteitä ovat (Kaspersky www sivut):

- Internet
- Sähköposti
- Sovellusten haavoittuvuudet
- Siirrettävät tallennuslaitteet
- Käyttäjien toiminta

Digitaalisia uhkia ja vaaroja ovat (Sanchez 2010):

- Haittaohjelmat (malware)
- Vakoiluohjelmat (spyware)
- Tietojen kalastelu (phishing)

- Väärennetyt tietoturvasovellukset
- Troijalaiset
- Virukset
- Madot
- Botnetit
- Rootkit

3.2.1 Digitaalisten uhkien lähteet

Internet on tuonut mukanaan paljon erilaisia tapoja hyökätä yritysten kimppuun ja uusia keinoja keksitään jatkuvasti. Siksi onkin tärkeää suojata yhteyksiä internetiin ja tunnistaa haavoittuvuuksia järjestelmissä. Ennen järjestelmiin pääsi käsiksi lähinnä pelkästään yrityksen sisäpuolelta, mutta nykyään yritysten järjestelmät ovat käytettävissä lähes mistä vain. Järjestelmien tulee olla hyvin suojattuja varsinkin, jos asiakkaat ovat myös järjestelmien loppukäyttäjiä. (Newman 2010, 24.)

Työntekijöitä pitää myös opettaa käyttämään digitaalisia yhteyksiä vastuullisesti ja määriteltyjen tietoturvasääntöjen mukaan. Töitä tehdessä kotoa käsin on myös osattava noudattaa yrityksen tietoturvapolitiikkaa. Sovellusten haavoittuvuudet tulee korjata mahdollisimman nopeasti niiden löytymisen jälkeen. (Newman 2010, 24.)

3.2.2 Digitaaliset uhat ja vaarat

Virukset, madot, troijalaiset, vakoiluohjelmat, väärennetyt tietoturvasovellukset ja rootkitit voidaan kaikki luokitella haittaohjelmiksi. Ne ovat pääasiassa sovelluksia, jotka ovat vihamielisiä, tunkeutuvia ja häiriköiviä. Tietoturvarikollisuudessa käytetään monia erilaisia tapoja yritysten tietojen kalasteluun tai työntekijöiden huijaamiseen. (Sanchez 2010.)

Botnetit ovat verkosto saastuneita tietokoneita, joita voidaan käyttää moniin eri tarkoituksiin. Saastunut tietokone voi näyttää aivan normaalilta ennen kuin sitä aletaan

käyttää rikolliseen toimintaan. Tietokoneen sijainnilla ei ole myöskään väliä niin kauan kuin tietokone on vain yhdistettynä internetiin, jonka kautta hakkeri voi lähettää komentoja saastuneelle tietokoneelle. Niiden avulla voidaan suorittaa erilaisia hyökkäyksiä kuten haittaohjelmien ja roskapostin lähettämistä, käyttää verkostoa tietojen varastamiseen ja tehdä DoS (Denial of Service) hyökkäyksiä. (Norton www sivut.)

Kaikilta näiltä asioilta voi suojautua käyttämällä hyviä tietoturvasovelluksia ja palomuureja. Käyttöjärjestelmiin tulee asentaa uusimmat tietoturvapäivitykset. Yhteyksiä voidaan myös suojata ja suodattaa erilaisilla tavoilla. Yleisesti internetin käytössä kannattaa olla varuillaan ja sähköposteja avatessa kannattaa olla availematta tuntemattomia liitetiedostoja. Internetiä ei kannata myöskään kannata selailla vanhentuneilla selainsovelluksilla. (McAfee www sivut.)

4 TURVAJÄRJESTELMÄT

Turvajärjestelmillä pyritään estämään mahdolliset rikokset ja havaitsemaan mahdollisia infrastruktuurin vikoja ajoissa. Siihen voidaan käyttää erilaisia osia, joista kootaan yritykseen tarvittava kokonaisuus. Jokaisen yrityksen tarpeet ovat erilaiset, mutta jokaisessa yrityksessä tulee olla edes perustason turvajärjestelmät kuten murtotunnistimet ovissa ja tarvittaessa laseissa.

Turvajärjestelmät kannattaa aina hankkia asiantuntevasta yrityksestä, varsinkin jos hankitaan erikoisempia turvallisuuslaitteita. Perustason laitteita pystyy asentamaan itsekin, mutta niiden tehokkuus voi olla heikompi kuin asiantuntevan yrityksen kanssa tehdyn turvallisuussuunnitelman mukaisesti asennetut laitteet.

4.1 Murtautumisen estäminen

Ovitunnistimet ovat hyvä ensimmäinen laite estämään murtautumisia. Tunnistimet ovat hyödyllisiä kaikkialla ensitason murronestona. Ikkunoita varten on myös mah-

dollista asentaa samanlaiset avaamista havaitsevat tunnistimet. Niitä varten voidaan myös asentaa tunnistimet, jotka havaitsevat, jos ikkunat menevät rikki. (SecuritySystemReviews www-sivut.)

Liikkeentunnistimet ovat myös hyvä tapa ehkäistä rikoksia. Kehittyneet liikkeentunnistimet osaavat jopa tunnistaa onko kyseessä esimerkiksi pienempi eläin, jolloin laite ei turhaan aktivoidu ja reagoi kaikkeen. Valvontakamerat ovat parhain tapa valvoa yrityksen tiloja. Ne voivat olla ’tyhmiä’ laitteita, jotka kuvaavat aluetta ja niiden talletuksia voidaan katsella erikseen, mutta valvontakamerat voivat olla myös katseltavissa esimerkiksi puhelimesta jatkuvasti internetin kautta. Tällöin aluevalvontaa voidaan suorittaa mistä vain ja milloin vain. (Rytmi Rakennus Oy www sivut.)

4.2 Infrastruktuurin viat

Vesivahinkoja varten on olemassa erilaisia valvonta ja automaatiojärjestelmiä. Putkia voidaan valvoa antureilla, jotka antavat hälytyksen heti, jos jokin putki alkaa vuotaa. (Rytmi Rakennus Oy www sivut.) Putkistoihin voidaan myös asentaa automaattisia sulkimia, jotka sulkevat veden, jos vuoto havaitaan (Derek 2014).

Yrityksessä olisi myös hyvä olla jonkinlaiset ylijännite suojat. Tällaisia voidaan asentaa suoraan sähkökeskukseen, joka estää pienemmät ylijännitteet sähköverkossa ja estää laitteita hajoamasta. Ukkosia vastaan on myös olemassa ukkosylijännitesuojia, mutta nämäkään eivät takaa ukkosen aiheuttamilta vahingoilta säästymistä. Parhaimpia suojia ukkosta vastaan on perinteinen tapa eli otetaan sähkölaitteet irti sähköverkosta. Puhelinjohdot ovat myös tärkeää ottaa irti, koska ukkonen tulee myös niitä pitkin. (Loiste www-sivut.)

Yrityksen tärkeimpiä laitteita olisi myös hyvä suojata Uninterruptable Power Source eli UPS-laitteella. Tällainen laite pitää sähkölaitteet hetkellisesti päällä sähkökatkon aikanakin, jonka aikana pystytään sammuttamaan laitteet turvallisesti ilman suuria tietojen menetyksiä. UPS-laite suojaa myös yli- ja alijännitteeltä. (Power Shield www-sivut.) Jotkin UPS-laitteet voidaan myös kytkeä laitteisiin datajohdolla, jolloin

ne osaavat automaattisesti tallettaa auki olevat työt sekä sammuttaa tietokoneen turvallisesti.

5 VERKKOJEN SUOJAAMINEN

5.1 Palomuuri

Palomuuri on erittäin tärkeä laite tietoturvan osa, joka on lähes pakollinen jokaisessa yrityksessä. Sen tehtävänä on suojata yritystä hyökkäyksiltä ja estää turhia yhteyksiä yrityksen verkkoon. Palomuuri voi olla asennettuna lähes jokaiseen laitteeseen sovelluksena. Tämä ratkaisu ei ole läheskään yhtä tehokas tapa kuin erillinen palomuurilaite, joka suojaa koko verkkoa. (TechAdvisory www-sivut.)

Palomuurilaite on tehokas suoja yrityksen verkolle, koska se on yleensä ensimmäinen tai toinen laite, joka on yhdistettynä internetiin. Palomuuri pystyy siis estämään vaaralliset yhteydet yrityksen verkon muihin laitteisiin ilman, että mahdollinen hyökkääjä saa mitään tietoa yrityksen laitteista. Palomuurilaitteissa on myös enemmän ominaisuuksia verrattuna sovelluspohjaiseen palomuuriin. Parhaimman suojan palomuurilaitteesta saa, kun se on tietoturvayrityksen hallittavissa etäyhteydellä, koska he voivat jatkuvasti tarkkailla palomuurin toimintaa. Yrityksen verkko on silloin suojattuna ympäri vuorokauden ja ammattilaiset pystyvät muokkaamaan suojausasetuksia tarvittaessa helposti. (TechAdvisory www-sivut.)

Palomuurisovellus on heikompi ratkaisu, koska vaarallinen yhteys pääsee laitteeseen asti ennen kuin palomuurisovellus estää sen. Tämä pienikin aika voi olla vaarallinen, koska siinä ajassa, kun palomuuri pyrkii estämään yhteyden, se on jo voinut saada aikaan jotain pahaa laitteessa. Tämä ratkaisu myös vaatii, että palomuurisovellus on asennettu jokaiselle laitteelle erikseen. Palomuurisovellus voi olla asennettuna kuitenkin palomuurilaitteen kanssa samanaikaisesti. Kannettavissa laitteissa sekä myös laitteissa, jotka sisältävät kriittistä tietoa, on suositeltavaa aina käyttää palomuurisovellusta. (TechAdvisory www-sivut.)

Hyviä palomuurilaitteen ominaisuuksia yrityksille ovat (Hughes, 2017):

- Virustorjunta
- Tunkeutumisen estopalvelu (Intrusion Prevention Service)
- Internetin suodatus
- Raportointi
- Virtuaaliset yksityiset verkot (Virtual Private Networks)
- Tekninen tuki

5.1.1 Modeemi

Modeemin tehtävä on internetiin yhdistäminen. Se toimii siltana palveluntarjoajan ja yrityksen välillä. Modeemit eivät sisällä suojauksia ja ne tekevät vain yhtä työtä eli yhdistävät internetiin. Usein kuitenkin palveluntarjoajat myyvät käyttäjille laitteita, jotka ovat modeemin ja reitittimen yhdistelmiä. Tällaiset yhdistelmälaitteet voivat sisältää suojausominaisuuksia.

5.1.2 Reititin

Reitittimen päätarkoitus on yrityksen langallisen verkon luominen ja mahdollisesti myös langattoman verkon luominen. Osa kalliimmista nykyaikaisista reitittimistä voi toimia kuitenkin myös yrityksen palomuureina, koska niihin on sisäänrakennettuna suojaustoimintoja. Reitittimet sisältävät yleensä vain perustason suojausominaisuuksia, joten ne toimivat varsinaista palomuurilaitetta heikompana suojana. (Hughes, 2017.)

5.2 Virustorjuntaohjelmisto

Virustorjuntaohjelmisto on yritykselle erittäin tärkeä. Se suojaa laitteita viruksilta ja haittaohjelmilta. Virustorjunta suojaa koneita niihin suoraan kytketyiltäkin laitteilta kuten muistitikuilta ja puhelimilta. Riippuen palveluntarjoajasta virustorjuntaohjelmiston pystyy asentamaan kaikille laitteille kuten tietokoneille, puhelimille, tableteille ja palvelimille. Virustorjunta suojaa yrityksen tiedostoja, sähköposteja ja virustor-

junta voi toimia jopa varastamisen suojana kannettavissa tietokoneissa ja mobiililaitteissa. (Stevens, 2016.)

Yrityksille suunnatut virustorjuntaohjelmistot ovat yleensä hintavia, mutta niitä saa yleensä hyvin räätälöidyissä paketeissa yrityskohtaisten tarpeiden mukaan. Virustorjuntaohjelmistoa valittaessa kannattaa mahdollisesti keskittyä helppokäyttöisyyteen ja yhtenäisesti hallittaviin vaihtoehtoihin, varsinkin jos yrityksessä ei ole kokoaikaista IT-työntekijää. (Stevens, 2016.)

5.3 Verkon jakaminen osiin

Yrityksen verkko voidaan jakaa osiin, jos halutaan erotella vaikkapa vierailijoiden laitteet yrityksen omista laitteista. Tällainen jaottelu lisää yrityksen verkon tietoturvaa, koska vierailijan mahdollisesta saastuneesta laitteesta ei pääse leviämään haittaohjelmia yrityksen omiin laitteisiin yhtä helposti. Suurempien verkkojen jakaminen kuitenkin lisää verkon hallitsemisen vaikeutta ja siihen voidaan tarvita paljon enemmän teknistä tietotaitoa ja kalliimpia laitteita. (Metivier, 2017.)

Verkko voidaan jakaa joko fyysisesti tai virtuaalisesti. Fyysinen jakaminen on vaikeampi ja kalliimpi toteuttaa, koska jokaisella jaetulla alueella on oma internetyhteytensä sekä oma palomuuri tai reitin laite. Jaetut alueet ovat siis fyysisesti eri verkkoja internetistä asti. Virtuaalisesti jaettu verkko taas käyttää yhtä internetyhteyttä. Verkoilla on silloin jaettu palomuuri tai reititin, joka voidaan jaotella eri osiksi käyttämällä kytkimiä, jotka muodostavat omia verkkojaan. (Metivier, 2017.)

5.3.1 Langattomat verkot

Langattoman verkon jakaminen on suhteellisen halpa toteuttaa, koska suurin osa palomuureista ja reitittimistä osaa luoda useampia turvallisia langattomia verkkoja. Yrityksen ei tarvitse siis laittaa paljoa rahaa kiinni tarjotakseen vierailijoilleen ylimääräistä mukavuutta. Vierailijoille tarkoitettu langaton verkko on melko helppo toteuttaa ja hallita.

Langattoman vierailijaverkon luomisessa kannattaa kuitenkin varmistaa, että laite osaa luoda salatun yhteyden, koska salaamaton yhteys voi olla haitallinen sen käyttäjille ja joissain tapauksissa jopa yritykselle. Salatun yhteyden tulisi käyttää vähintään WPA2-salausta. (Ubiquiti Networks www-sivut.)

5.3.2 Langalliset verkot

Verkossa olevat kytkimet voidaan jaotella omiksi verkoikseen, jotka voivat olla kooltaan suuria tai pieniä. Langallisen verkon jakamisella voidaan esimerkiksi erotella palvelimet ja työkoneet toisistaan, joka lisää molempien tietoturvaa, koska ne eivät ole suoraan yhteydessä toisiinsa. Verkon jakaminen pienempiin osiin myös vähentää rasitusta verkon sisällä, koska yhdessä verkossa ei ole liian montaa laitetta kommunikoimassa keskenään. (InfoSec Institute www-sivut.)

Yrityksen palomuuri tai reititin saattaa kuitenkin rasittua liikaa, jos verkossa on monta pienempää verkkoa ja paljon laitteita. Jokainen laite verkossa lähettää palomuurille tai reitittimelle pyyntöjä tiedon siirtämiseen, joka rasittaa palomuurilaitetta. Tämän takia verkon avuksi voidaan hankkia tarpeeksi tehokas palomuuri tai reititinlaite ja mahdollisesti lisäavuksi voidaan käyttää erillisiä palvelimia, jotka hoitavat osan näiden laitteiden taakasta. (InfoSec Institute www-sivut.)

5.4 Virtual Private Network

Virtual Private Network eli VPN mahdollistaa työntekijöiden turvallisemman työskentelyn etäisesti. Yrityksen palomuurin tai reitittimen tulee osata ottaa vastaan VPN-yhteyksiä, joka mahdollistaa turvallisen ja salatun yhteyden luomisen yrityksen verkon ja käyttäjän välillä. Käyttöjärjestelmät itsessään yleensä sisältävät työkalut VPN-yhteyden luomiseen. Yhteyden luomiseen voidaan käyttää myös erillisiä sovelluksia ja joissain tapauksissa ne voivat olla vaadittujakin. VPN-sovelluksia löytyy ilmaisista sovelluksista maksullisiin sovelluksiin. (Richmond, 2012.)

Yrityksen työntekijän oma laite tulisi kuitenkin olla aina yhtä suojattu kuin työpaikan omat laitteet ja verkko ovat. Parhain toimintatapa työntekijöiltä olisi, jos he eivät

käyttäisi etälaitteitaan sähköpostin lukemiseen tai internetin selailuun. Tämä ei kuitenkaan ole yleensä mahdollista ja työntekijät tulisi kouluttaa käyttämään etätyölaitteitaan mahdollisimman turvallisesti. Työntekijöiden tulisi asentaa kaikki uusimmat turvapäivitykset ja pidettävä koneensa puhtaana haittaohjelmista. Käyttäjien tulisi myös valita laitteisiin vahvoja salasanoja ja käyttää eri salasanoja kotona kuin yrityksen järjestelmissä. (Richmond, 2012.)

6 TIEDON SUOJAAMINEN

6.1 Käyttöjärjestelmien ja sovellusten päivittäminen

Yleisesti kaikkien ohjelmistojen päivittäminen on tärkeää nykypäivänä. Päivitykset auttavat suojaamaan käyttäjiä tietoturvauhilta. Joka päivä löydetään uusia haavoittuvuuksia järjestelmistä, jotka on hyvä korjata mahdollisimman nopeasti, kun päivitys on saatavilla. Automaattisia päivityksiä on hyvä käyttää varsinkin käyttöjärjestelmien päivityksissä. Joitain sovelluspäivityksiä voi siirtää myöhemmäksi, jos ne eivät sisällä suojauspäivityksiä, mutta nekin on hyvä asentaa heti kun mahdollista.

Käytettävää käyttöjärjestelmää on myös syytä päivittää uuteen, jos vanhan käyttöjärjestelmän tukeminen on lakkautettu. Käyttöjärjestelmän haavoittuvuuksia ei pysty korjaamaan, jos käyttöjärjestelmälle ei enää tehdä suojauspäivityksiä. Joissain tapauksissa käyttöjärjestelmän uusiminen ei kuitenkaan ole niin tärkeää. Esimerkiksi jos konetta ei kytketä verkkoon lainkaan ja sitä käytetään täysin eristettynä internetistä. Jotkin vanhat ohjelmat voivat myös vaatia vanhempaa käyttöjärjestelmää toimiakseen, mutta tällaisetkin koneet on hyvä pitää irti yrityksen verkosta ja internetistä.

6.2 Varmuuskopiointi

Varmuuskopiointi on monille yrityksille välttämätöntä, koska yritys ei pysty mahdollisesti jatkamaan toimintaansa lainkaan, jos menetettyä tietoa ei pystytä palauttamaan edes osittain. Varmuuskopioita on hyvä ottaa yrityksen tärkeistä tiedoista päivittäin.

Tällä varmistetaan, että menetetään mahdollisimman vähän yrityksen tärkeitä tietoja ja vältetään työntekijöiden työpanoksen menetystä yrityksessä. Yrityksen tietojen palauttamisessa varmuuskopiosta kestää kuitenkin aikaa, joten isommissa järjestelmissä on myös hyvä keskittyä tietojen palauttamisen yksinkertaisuuteen. (Leonard, 2016.)

Tiedon kopioita on hyvä olla vähintään kolme. Ensimmäinen on tietenkin käytössä oleva kopio, jota käytetään työn tekemiseen ja sitä päivitetään päivän aikana. Toisena on paikallinen varmuuskopio, josta voidaan helposti ja nopeasti palauttaa yrityksen uusimmat tiedot. Kolmantena kopiona on hyvä pitää jossain muualla säilytettyä kopiota tiedoista. Tämä kolmas varmuuskopio voi olla ulkoinen kiintolevy, erillinen palvelin toisessa yrityksen toimistossa tai kopio voi olla vaikkapa pilvipalvelussa. (Leonard, 2016.)

6.2.1 NAS-laitteet

NAS eli Network Attached Storage tarkoittaa laitteita, jotka ovat liitettynä suoraan yrityksen verkkoon ja toimivat tiedostopalvelimina yrityksen muille laitteille. NAS-laitteet voivat toimia monina erilaisina ratkaisuina yritykselle, kuten isoina tallennustiloina sekä RAID-järjestelminä lisäten kiintolevyjen vikasietoisuutta tai luku- ja kirjoitusnopeutta. Ne ovat vähän kuin yrityksen sisäisiä pieniä pilvipalvelimia, jotka toimivat paljon tehokkaammin kuin internetin välityksellä toimivat pilvipalvelut. (Gewirtz, 2017.)

6.2.2 Nauha-asemat

Nauhakasetit ovat vieläkin hyvä tapa säilyttää tietoja. Nauhat eivät kuitenkaan sovellu jokapäiväiseen käyttöön, koska ne ovat hitaita etsimään tiettyjä tietoja. Nauhoille talletetaan tietoa samalla tavalla kuin videokasetille, joten tietyn tiedon löytämistä varten nauha kelataan oikeaan kohtaan, ennekuin se voidaan lukea. Nauhat tarjoavat suuria tallennustiloja suhteellisen halvalla, mutta niillä on aika korkeat käyttöönotto hinnat. Pitkäaikaisesti ja suurissa määrissä ne ovat kuitenkin edullisia. (PivotStor www-sivut.)

6.2.3 Pitkäaikainen säilytys

Pitkäaikaiseen säilytykseen parhaimpia välineitä ovat optiset levyt, jotka ovat tarkoitettu pitkäaikaiseen säilytykseen. Aivan tavalliset optiset levyt kestävät pitkään, mutta todella pitkäaikaiseen säilytykseen tarkoitetut levyt kestävät hyvissä oloissa säilytettynä parhaimmillaan jopa tuhat vuotta. Halvemmat pitkäaikaiseen säilytykseen tarkoitetut optiset levytkin kestävät yli 100 vuotta. Optisten levyjen kirjoitus- ja lukunopeudet ovat kuitenkin aika hitaita, joten niiden käyttäminen ei ole aina tehokasta. (Jacobi, 2016.)

Eri vaihtoehtoina pitkäaikaiseen säilytykseen ovat HDD ja SSD -levyt. Näiden kesto on kuitenkin rajoitettu pisimmillään kymmeneen vuoteen oikein säilytettynä ja huollettuna, joten niiden tiedot tulee välillä siirtää uuteen laitteeseen. Luku- ja kirjoitusnopeudet näissä laitteissa ovat kuitenkin paremmat kuin optisissa levyissä, joten niiden käytettävyys on myös tehokkaampaa. (Jacobi, 2016.)

Nauhakasetit ovat myös hyvä tapa säilöä tietoa pitkään. Nauhat kestävät jopa 30 vuotta oikein säilytettynä ja huollettuna. Ne ovat oikeassa käytössä hyvin kestäviä ja niiden vikasietoisuus on korkea. Nauhojen hinta on suhteellisen halpaa verrattuna kiintolevyihin, mutta nauha-asemat jotka niitä lukevat ovat kalliita. Nauhat ovat siis hyvä vaihtoehto pitkäaikaiseen talletukseen, jos niitä halutaan käyttää pitkään ja talletettavaa tietoa on paljon. (StorageSwiss www-sivut.)

6.3 Tiedon salaaminen

Salaus on tehokas tapa estää laite- ja tiedostovarkaita saamasta yrityksen tietoja haltuunsa. Yritykset voivat salata tiedostoja yksittäisesti tai koko kiintolevy kerrallaan. Ulkoisia medioita ja mobiililaitteita voidaan myös suojata salauksella. Tietokoneiden käyttöjärjestelmät itsessään sisältävät työkaluja joilla voi salata kiintolevyjä ja tiedostoja. Salaukseen on saatavilla kuitenkin monia ilmaisia ja maksullisia sovelluksia erilaisilla ominaisuuksilla. (Like Geeks www-sivut.)

Koko kiintolevy voidaan lukita salauksen taakse, joka vaatii erillistä salauksenpurkuun tarkoitettua salasanaa aina kun kone käynnistetään. Salasanan syötön jälkeen koko kiintolevyn tiedot ovat salaamattomia niin kauan kuin kone on päällä. Koko kiintolevyn salaus voidaan kuitenkin toteuttaa niinkin, että salaus on jatkuvaa ja kaikki tiedot ovat salattuja jatkuvasti, kun konetta käytetään. Jatkuva salaus kuitenkin hidastaa laitteen luku- ja kirjoitusnopeutta, koska laite joutuu purkamaan salauksen jokaisesta tiedostosta silloin kun se on käytössä ja salaamaan tiedoston uudestaan, kun sitä ei käytetä. Ulkoiset mediat on aina hyvä pitää jatkuvasti salattuina, kuten myös mobiililaitteet. (Symantec 2015, 5.)

Koko kiintolevyn salauksen sijaan voidaan käyttää vain osittaista salausta, jossa salataan vain tietyt tiedostot. Yksittäisiä tiedostoja voidaan salata erikseen tai salata kokonainen kansio, jonka sisällä olevat tiedostot salataan. Tiedostot ja kansiot, jotka ovat salattuja, pysyvät salattuina, vaikka niitä siirrettäisiin tai kopioitaisiin. Yksittäisten tiedostojen ja kansioiden salaaminen on tehokas tapa jakaa tietoja muiden ihmisten välillä, jos halutaan taata, etteivät väärät ihmiset saa tietoja haltuunsa. (Symantec 2015, 6.)

6.4 RAID-järjestelmät

RAID-järjestelmät antavat yrityksen kiintolevyjärjestelmille joko lisää vikasietokykyä tai luku- / kirjoitusnopeutta sekä joissain tapauksissa lisää käytettävää tilaa. Luku- ja kirjoitusnopeutta luodaan jakamalla tietoja monien kiintolevyjen välillä, joista voidaan samanaikaisesti lukea ja kirjoittaa tietoja. Vikasietoa saadaan taas peilaamalla yhden kiintolevyn tiedot toiselle kiintolevylle. Jotkin RAID-järjestelmät tekevät vain yhtä tai toista kun taas paremmat ja kalliimmat ratkaisut tuovat useampia etuja kerralla. RAID 0, 1, 5, 6 ja 10 ovat yleisesti hyödyllisimmät RAID-järjestelmät pk-yrityksille. (Chu, 2015.)

RAID 0 vaatii minimissään kaksi kiintolevyä. Se jakaa tiedostot kaikkien kiintolevyjen kanssa ja tuottaa luku- ja kirjoitusnopeutta kiintolevyille halvimmalla tavalla. Sen huonoin puoli on kuitenkin, että se ei lisää vikasietoa yhtään. Kun yksikin kiintolevy

hajoaa, niin kaikki tiedot menetetään. Tämä järjestelmä on hyödyllinen, kun halutaan halvalla luku- ja kirjoitusnopeutta johonkin järjestelmään ja tiedon menetyksestä ei ole suuria haittoja tai se saadaan palautettua varmuuskopiosta. (Ascenzo, 2016.)

RAID 1 taas halvin tapa saada kiintolevyille vikasietoisuutta, mutta se ei lisää luku- tai kirjoitusnopeutta yhtään. Tämä järjestelmä vaatii vähintään 2 kiintolevyä. Kiintolevyt peilaavat toisiaan eli sisältävät samat tiedot jatkuvasti. Tiedot kadotetaan vain silloin kun järjestelmän kaikki kiintolevyt ovat rikki samanaikaisesti. (Ascenzo, 2016.)

RAID 5-järjestelmä tuottaa lukunopeutta ja vikasietoisuutta. Se vaatii vähintään 3 kiintolevyä toimiakseen. Kaikki järjestelmän kiintolevyt takaavat toistensa yhtenäisyyttä. Tämä järjestelmä lisää kirjoitusnopeutta vain jonkin verran, koska kiintolevyille kirjoitetaan jatkuvasti myös yhtenäisyystietoja. Järjestelmän palautuminen kiintolevyn hajoamisesta on jonkin verran hidasta. RAID 5 kestää yhden kiintolevyn hajoamisen. (Chu, 2015.)

RAID 6 on periaatteessa täysin samanlainen järjestelmä kuin RAID 5, mutta se kestää kahden kiintolevyn samanaikaisen hajoamisen. Se siis tuottaa enemmän vikasietoisuutta. Tämä järjestelmä lisää lukunopeutta kiintolevyille, mutta se myös hidastaa kirjoitusnopeutta, koska usealle kiintolevylle joudutaan kirjoittamaan enemmän yhtenäisyystietoja jatkuvasti. Järjestelmän palautuminen kiintolevyn tai kiintolevyjen hajoamisesta on vielä hitaampaa kuin RAID 5:ssä. (Chu, 2015.)

RAID 10 on yhdistelmä RAID 0 ja RAID 1-järjestelmiä. Tämä toteutus tuottaa luku- ja kirjoitusnopeutta sekä vikasietoisuutta. Se on myös kallein järjestelmä, koska se vaatii vähintään 4 kiintolevyä ja tilan lisääminen vaatii aina vähintään 4 uutta kiintolevyä. Tämä järjestelmä siis yksinkertaisesti sanottuna jakaa tietoja kahden kiintolevyn välillä, joka samanaikaisesti peilataan kahdelle muulle kiintolevylle, jolloin tiedot säilyvät, vaikka toinen kiintolevy pari hajoaisi. (Chu, 2015.)

RAID-järjestelmiä voi luoda suoraan tietyillä käyttöjärjestelmillä, kuten Windows käyttöjärjestelmillä, mutta RAID-laitteiden käyttö antaa paremmat ominaisuudet RAID-järjestelmien luontiin ja hallitsemiseen. Tällaisia laitteita ovat esimerkiksi

RAID-laajennuskortit, kiintolevylaatikot sekä NAS-laitteet, jotka liitetään suoraan verkkoon erillisinä laitteina. (Chu, 2015.)

6.5 Salasanat

Salasanat ovat tärkeä osa yrityksen tietoturvaa. Yrityksen työntekijät tulisi opettaa luomaan vahvoja salasanoja, joita ei ole helppo arvata tai murtaa. Jokaisella järjestelmällä ja palvelulla tulisi olla oma salasanansa ja työntekijän ei tulisi käyttää samoja salasanoja kotona ja työpaikalla. (National Cyber Security Centre www-sivut.)

Salasanaa vaihtamalla estetään luvatonta salasanan käyttöä, jos salasana on päässyt jonkun käsiin fyysisesti. Se ei suojaa niin paljoa hyökkääjiltä, koska jos hyökkääjä on onnistunut saamaan yhteyden järjestelmään, hän on voinut asentaa järjestelmään takaovia tai muita ratkaisuja, jotka täysin mitätöivät salasanan vaihdon hyödyn. Salasanan vaihtaminen on hyödyllistä niissä tilanteissa, kun salasana on joutunut tai sen epäillään joutuneen luvattomiin käsiin. (Chiasson, van Oorschot. 2015, 5.)

Salasanojen jatkuvassa vaihtamisessa on muitakin haittapuolia. Käyttäjät itse keksivät salasanansa ja kun he joutuvat usein vaihtamaan salasanaansa, alkavat uudet salasanat olla täysin samanlaisia kuin vanhat salasanat. Esimerkiksi jos käyttäjän vanha salasana oli ’Salasana1’ hän saattaa valita uudeksi salasanakseen ’Salasana2’, joka on helposti murrettavissa ja jopa arvattavissa. (Zhang, Monrose, Reiter. 2010, 9.)

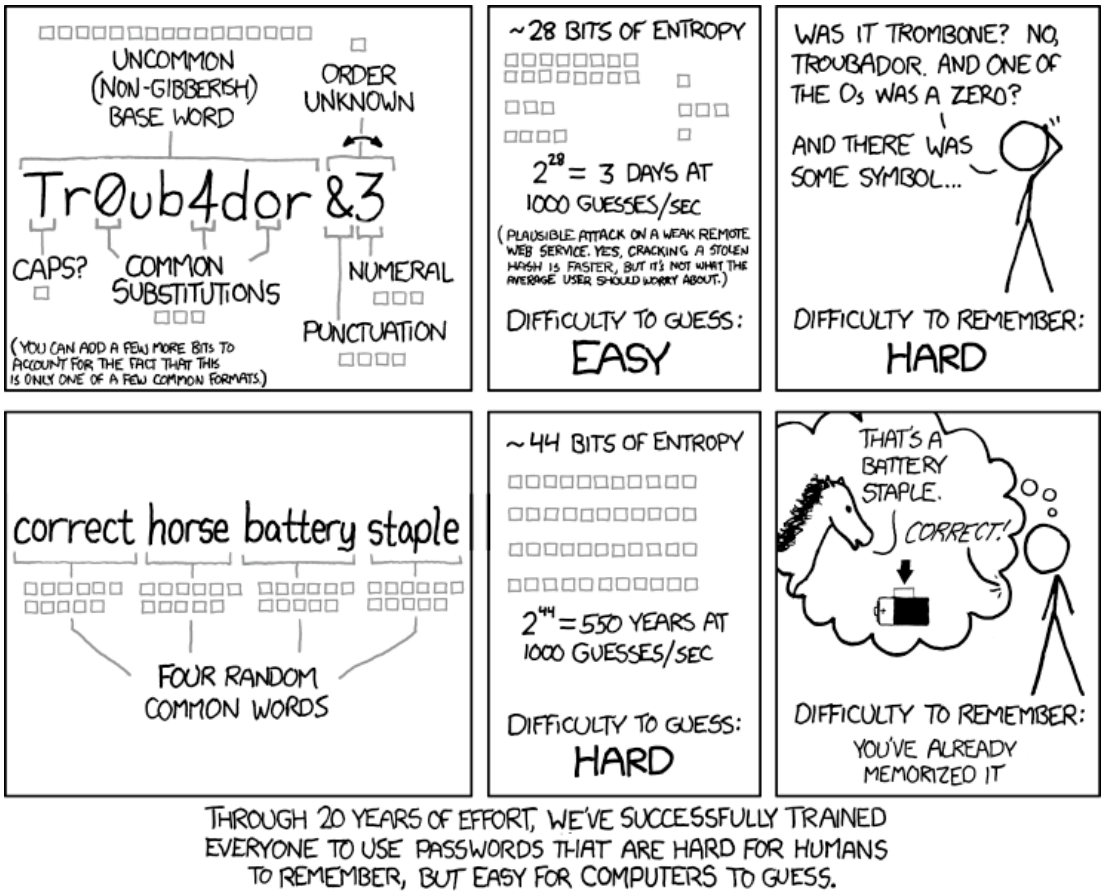
Tärkeimpiä salasanoja yrityksessä ovat järjestelmänvalvojien tilien salasanat, joiden täytyy olla hyvin valittuna. Järjestelmänvalvojilla tulisi olla myös normaalikäyttöön tarkoitettu tili eri salasanalla ja heidän ei tulisi käyttää järjestelmänvalvojan tiliä turhaan. Laitteiden oletus-salasanojen vaihtaminen on myös erittäin tärkeää, koska ne ovat helposti arvattavissa, murrettavissa tai jopa julkista tietoa. (National Cyber Security Centre www-sivut.)

6.5.1 Vahvan salasanan valitseminen

Vahvojen salasanojen valitseminen on erittäin tärkeää, koska salasanat ovat usein heikoin lenkki tietoturvassa. Valitsemalla vahvoja salasananoja vähennetään tietoturvariskiä ja estetään luvaton laitteiden ja järjestelmien käyttö. Salasanojen tulisi olla mahdollisimman vaikeasti arvattavia ja monimutkaisia, mutta kuitenkin helposti muistettavia. Käyttäessä useita salasanoja voidaan avuksi ottaa salasanojen hallinta ohjelmia, jotka säilyttävät salasanat yhden salasanan takana. (Moramarco, 2017.)

Ennen suositeltiin, että salasanan tulisi olla tarpeeksi pitkä ja sisältää vähintään yhden iso kirjaimen, yhden numeron ja yhden erikoismerkin sekä salasanoja tulisi vaihtaa 30, 60 tai 90 päivän välein lisätäkseen tietoturvaa. Tämä ei pidä enää täysin paikkaansa. Tämän suosituksen alkuperäinen kirjoittajakin on myöntänyt, että tämä ei lisää salasanan suojausta paljoa, koska ihmiset keksivät liian arvattavissa olevia yhdistelmiä. (May, 2017.)

Tästä kaikesta huolimatta salasanan tulisi olla vähintään 15-20 merkkiä pitkä ja sisältää joitain erikoismerkkejä. Salasanan valitsemiseen voi myös käyttää aivan normaaleja sanoja, kunhan ei valitse liian tavallisia sanoja, eikä käytä niitä normaalina lauseena. Esimerkkinä alla (kuva 4) on tapoja valita suhteellisen hyviä salasanoja, mutta esimerkkiä ei kannata ottaa liian kirjaimellisesti ja kaikkiin salasanoihin on hyvä sisällyttää ainakin joitain erikoismerkkejä. (The University of Edinburgh www-sivut.)



Kuva 4. Salasanan valitsemisen vaihtoehtoja. (Munroe, 2011.)

6.5.2 Salasanojen hallinta, säilytys ja suojaus

Salasanoja on yleensä käytössä monia samanaikaisesti ja ne ovat välillä vaikeasti muistettavia. Näiden syiden takia yrityksen onkin hyvä harkita käyttävänsä salasanojen hallintaohjelmia. Tällaiseen ohjelmaan voidaan säilöä yrityksen salasanoja ja pitää ne mahdollisimman turvattuina. Hallintaohjelmat auttavat käyttäjiä käyttämään pitkiä ja monimutkaisia salasanoja. Nämä ohjelmat voivat luoda myös salasanoja käyttäjän puolesta. Salasanojen hallintaohjelmasta voidaan käydä hakemassa tarvittavan järjestelmän salasana ja jotkut hallintaohjelmat osaavat jopa syöttää joihinkin järjestelmiin oikean salasanan automaattisesti helpottaen käyttöä. (Emma W, 2017.)

Hyvät hallintaohjelmat tarjoavat muitakin tietoturvasuojia. Ne voivat tunnistaa huijaussivustoja ja tarjoavat huomautuksia uusista mahdollisista huijausyrityksistä. Joitain hallintaohjelmia voi myös synkronoida useiden laitteiden välillä, joka helpottaa liikkuvaa työntekijää. Muina hyödyllisinä etuina hallintaohjelmilla on heikkojen tai

uudelleen käytettyjen salasanojen muistutukset ja varoitukset, vanhojen salasanojen vaihtamisen muistutukset, sekä monitasoiset tunnistautumiset. Salasanojen hallintaohjelmat tulisi olla salatulla asemalla tai niiden tiedostot tulisi olla salattuina. Kannettavissa laitteissa, joissa on salasanoja, tulisi aina olla salattuna. (Emma W, 2017.)

Salasanojen hallintaohjelmilla on kuitenkin huonojakin puolia. Tällainen hallintaohjelma vaatii kuitenkin yhden muistettavan salasanan ja tämän salasanan tulisi olla mahdollisimman monimutkainen. Salasanan muistamista voidaan kuitenkin helpottaa käyttämällä tunnuslausetta vaikeasti muistettavan salasanan sijaan. Salasanojen hallintaohjelman salasanan varastaminen tarkoittaa, että varas saa haltuunsa kaikki yrityksen salasanat kerralla. Toisena ongelmana on salasanan unohtaminen, joka myös johtaa kaikkien salasanojen menettämiseen. Hallintaohjelman salasanan voi kirjoittaa paperille tarvittaessa, mutta se tulee säilyttää lukitussa säiliössä. (Emma W, 2017.)

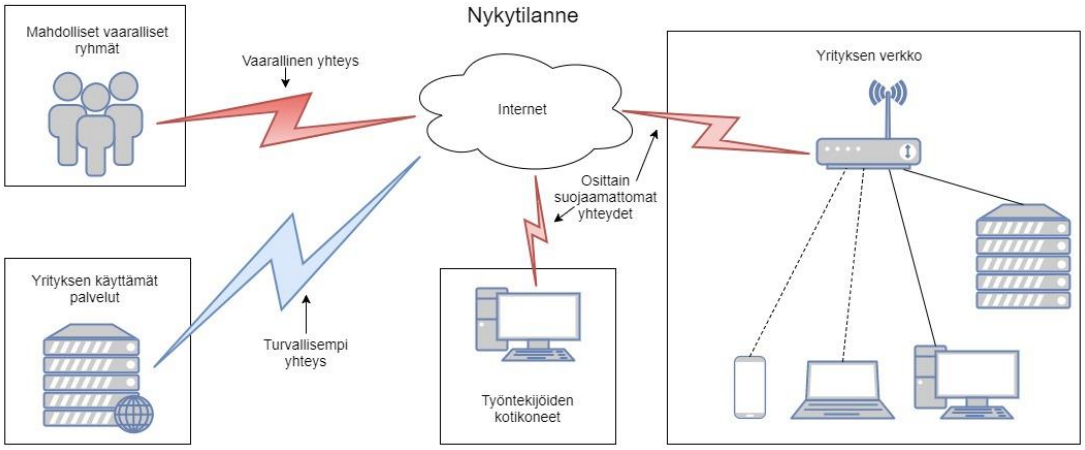
7 MIKROYRITYKSEN MÄÄRITELMÄ

Suomessa on todella paljon mikroyrityksiä. Yli 90% suomalaisista yrityksistä on mikroyrityksiä. Tällaisen yrityksen määritelmä on, että sillä on alle 10 työntekijää. (Yrittäjät www-sivut.) Suomessa kirjanpidon osalta mikroyrityksillä on kolme eri määrittelevää raja. Yrityksen liikevaihto ylittää 700 000 euroa, taseen loppusumma on 350 000 euroa tai yrityksellä on palveluksessaan tilikauden aikana keskimäärin 10 työntekijää. Yritys määritellään mikroyritykseksi, kun yksikin näistä rajoista ylitetään. (Taloushallintoliiton www-sivut.)

8 YRITYKSEN KUVAUS

Yritys on pieni liike, jossa on alle 10 työntekijää. Heillä on käytössään vain muutama pöytäkone, yksi palvelin, pari kannettavaa ja joitain henkilökohtaisia laitteita. Yritys hyödyntää ulkopuolisia palveluita, joihin otetaan yhteys internetselaimen kautta.

Työntekijät voivat tehdä töitä kotoa käsin henkilökohtaisilla tietokoneillaan, mutta pääasiassa työnteko tapahtuu yrityksen laitteilla yrityksen verkossa. Työntekijöiden tietoturvaosaaminen on vaihtelevaa, mutta yleinen taso on heikko.



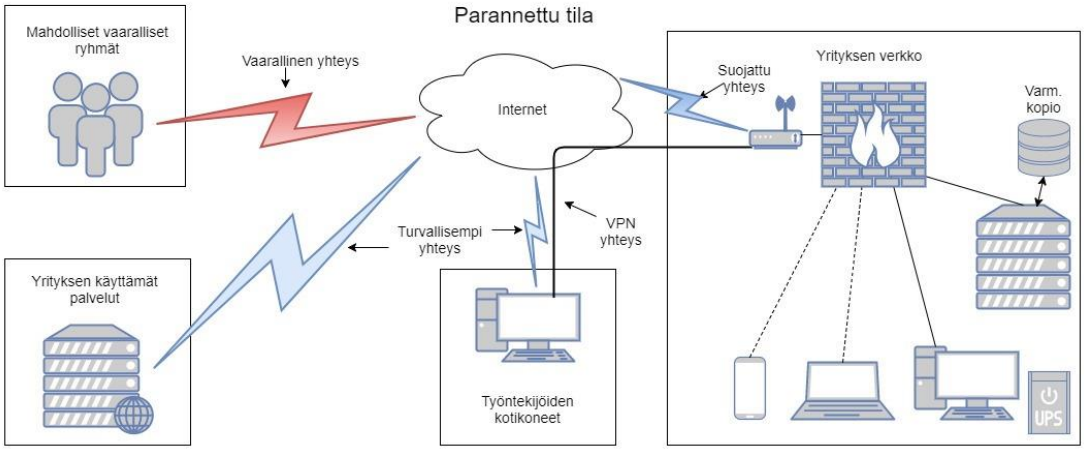
Kuva 1. Yrityksen verkon nykytila.

Yrityksellä on käytössään jo valmiiksi virustorjuntaohjelmisto ja sovelluspohjainen palomuuri tietokoneissaan käytössä. Yritys yhdistää internetiin halvalla palveluntarjoajan reitittimellä, jossa on joitain suojausominaisuuksia käytössä. Heidän palvelimensa käyttää kahden kiintolevyn RAID 1 ratkaisua varmuuskopiointiin ja osa tiedoista varmuuskopioidaan silloin tällöin ulkoisille medioille. Yritys käyttää paljon ulkopuolisia resursseja, joten paikallisen tiedon määrä ei ole suuri. Työntekijöillä ei ole mahdollisuutta käyttää yrityksen resursseja etätyötä tehdessä, joten etätyön tekeminen rajoittuu ulkopuolisten palvelujen käyttöön. Yrityksen langaton verkko on suojattu WPA2 AES-salauksella, mutta langattomia verkkoja on vain yksi. Asiakkaat, jotka haluavat käyttää yrityksen langatonta verkkoa saavat siis yhteyden yrityksen sisäiseen verkkoon, jos yritys jakaa heille salasanansa. Liikkeen tilat ovat suojattuna ovissa ja ikkunoissa olevilla murtohälyttimillä. Yrityksessä on myös palohälytinjärjestelmä ja vaahtosammutin.

8.1 Yrityksen tietoturvan parannustarpeet

Yrityksen tarvitsee alkaa suojata paremmin verkkoaan, koska kaikki laitteet eivät ole suojattuna tarpeeksi hyvin. Reititin tulisi vaihtaa palomuurilaitteeksi tai paremmaksi

reititin laitteeksi, joka tarjoaa palomuurin ominaisuuksia. Varmuuskopiointi tulisi myös suorittaa paremmin, koska se on vain osittain ratkaistuna tällä hetkellä ja varmuuskopiointi ei ole riittävän pitkäkestoisesti suunniteltua. Yrityksen tärkeitä tietoja tulisi myös alkaa salata. Työntekijöiden tulisi yhdistää työpaikan verkkoon suojatulla VPN-yhteydellä. Yrityksen langaton verkko tulisi jakaa kahteen osaan, joista toinen on yrityksen sisäisessä käytössä ja toinen vierailijoiden käyttötarpeita varten oleva. Yrityksen liiketiloja voisi suojata paremmin erilaisilla infrastruktuurin vikojen tunnistimilla ja mahdollisesti kameravalvonnalla. Yrityksen työntekijöitä tulisi myös kouluttaa tietoturvan osalta, koska heidän osaamisensa on vähäistä. Koulutus auttaisi myös työntekijöitä turvaamaan kotikoneensa paremmin, joka vähentäisi tietoturvariskiä. Näillä muutoksilla saadaan yrityksen tiedot paremmin turvattua ja pidettyä mahdolliset riskitekijät kurissa.



Kuva 2. Toivottu parannettu tila.

9 TIETOTURVAMUUTOKSET YRITYKSEEN

Mielikuvitukselliseen yritykseeni tullaan ensimmäisenä hankkimaan palomuurilaite yhteyksien suojaamiseksi. Yritykseen hankitaan halpa palomuurilaite, jossa tulee mukana lisenssit vuoden virustorjuntaan, sisällönsuodatukseen, sovellusvahtiin ja roskapostinsuodatukseen. Lisenssien jatkamista suositellaan tulevaisuudessa, mutta se jätetään toimitusjohtajan päätettäväksi. Palomuurissa on tuki VPN-yhteyksille ja

muita yleisiä suojaustoimintoja kuten esimerkiksi hyökkäyksien esto ja pakettien tarkastelu. Yrityksen tiedonsiirtotarve ei ole suuri, joten halvempi palomuurilaite, joka sisältää kuitenkin tarvittavat ominaisuudet, on tarpeeksi tehokas ratkaisu yritykselle. Palomuuri tulee olemaan toinen laite yrityksen verkossa ja se tulee toimimaan myös reitittimenä sekä Wi-Fi-laitteena. Työntekijät voivat yhdistää yrityksen verkkoon L2TP IPSec VPN-yhteydellä. Tämän VPN yhteyden pystyy muodostamaan helposti suoraan kotikoneen käyttöjärjestelmän sisäänrakennetuilla ominaisuuksilla ja se antaa koko yrityksen verkon käyttöön kotoa käsin.

Yrityksen käytössä oleva virustorjunta on jo tarpeeksi hyvä ratkaisu yrityksen kokoon nähden, joten sitä ei tarvitse vaihtaa toiseen. Yrityksen käytössä on myös jo valmiiksi kaikille tietokoneille asennetut sovelluspohjaiset palomuurit, jotka on hyvä jättää käyttöön siltä varalta, että palomuurilaite saattaa hajota jossain vaiheessa. Sovelluspohjaisten palomuurien käyttö ei myöskään haittaa laitteiden käytettävyyttä. Palomuurisovellus on myös hyvä, jos kannettavia laitteita käytetään yrityksen verkon ulkopuolella.

Langaton verkko jaetaan kahteen osaan, joista toinen toimii vierasverkkona. Vieraille tarkoitettu verkko on eristettynä yrityksen työntekijöiden käytössä olevasta langallisesta ja langattomasta verkosta. Vierasverkko käyttää WPA2 AES-salausta ja sen salasana on vapaassa jaossa yrityksen asiakkaille. Vierasverkon nopeutta ei kuitenkaan rajoiteta, koska se on asiakkaiden käytössä hyvin vähän. Yrityksen työntekijöiden käytössä oleva langaton verkko käyttää eri salasanaa ja se on myös suojattu WPA2 AES-salauksella. Langallisen verkon jakaminen ei ole tarpeellista, koska yrityksen käytössä on vain muutamia laitteita ja jakaminen ei tuo juurikaan mitään hyötyä yritykselle. Langallisen verkon jakaminen vain lisäisi yrityksen verkon hallitsemisen monimutkaisuutta. Yrityksen asiakkaiden laiteita ei tulisi ikinä liittää yrityksen langalliseen verkkoon tai muihin yrityksen laitteisiin tietoturvariskien välttämiseksi.

Yritykseen hankitaan myös varmuuskopiointia varten laite, joka hoitaa varmuuskopiointia tärkeästä tiedosta. Laitteen ei tarvitse olla kallis, koska sitä käytetään pääasiassa varmuuskopioinnin säilyttämiseen ja siitä voidaan palauttaa menetetyt tiedot tarvittaessa. Tähän tehtävään hankitaan kahden kiintolevyn NAS-laite, joka käyttää RAID 1-järjestelmää varmuuskopion hajoamisen varalta. Yrityksen kaikki tärkeät

tiedot talletetaan palvelimelle, joten työntekijöiden tietokoneiden tiedostoja ei tarvitse varmuuskopioida. Yrityksen tiedon määrä on vähäistä, joten varmuuskopio on hyvä ottaa kaikesta tiedosta palvelimella. Tähän tehtävään voidaan hankkia ilmainen varmuuskopiointiohjelma tai käyttää Windowsin omaa varmuuskopiointia, joka ottaa päivittäin samaan aikaan kopion yrityksen palvelimesta. Kolmatta varmuuskopiota varten hankitaan ulkoinen kiintolevy, johon otetaan varmuuskopiot tärkeistä tiedoista kerran kahdessa viikossa tai useammin, jos lyhyemmässä ajassa on tapahtunut paljon tärkeitä muutoksia. Kolmatta kopioita säilytetään toimitusjohtajan määrittämässä paikassa yrityksen tilojen ulkopuolella. Pitkäaikaisia varmuuskopioita otetaan polttamalla tärkeitä tietoja ja projekteja dvd-levyille.

Yritykseen laitetaan käyttöön myös tietojen salaus. Tämä toteutetaan käyttämällä ilmaista salausohjelmaa, joka tarjoaa hyvää salausta ja sen käyttäminen ei ole liian monimutkaista. Ratkaisuna käytetään koko kiintolevyn jatkuvaa salausta, koska käytettävän tiedon määrä ei ole suurta, joten koneiden käyttö ei hidastu liikaa.

Salasanojen käyttöä tehostetaan ja vanhat huonommat salasanat vaihdetaan uusiin parempiin salasanoihin. Salasanoja luodessa työntekijöiden tulee noudattaa yrityksen uutta salasanapolitiikkaa. Salasanojen tulee olla vähintään 16 merkkiä pitkiä. Niiden tulee myös sisältää vähintään yhden ison kirjaimen, numeron sekä erikoismerkin. Vaihtoehtoisesti salasanan sijaan voidaan käyttää tunnuslausetta, jonka tulisi koostua vähintään neljästä mahdollisimman erikoisesta sanasta, jotka eivät muodosta myöskään järkevää lausetta. Tähän tunnuslauseeseenkin tulee sisällyttää ainakin yksi iso kirjain, numero sekä erikoismerkki. Ulkopuolisia palveluita käytettäessä tulee kuitenkin myös huomioida heidän asettamansa vaatimukset ja rajat salasanojen luomisessa. Salasanojen jatkuvaa vaihtamista ei pakoteta, mutta salasanojen vaihtamista edes puolen vuoden välein suositellaan. Salasana tulee kuitenkin vaihtaa heti, jos sen epäillään joutuneen vääriin käsiin.

Toisena vaihtoehtona voidaan käyttää salasanojen hallintaohjelmalla luotuja salasanoja silloin kun mahdollista, koska salasanoja aletaan myös säilyttää salasanojen hallintaohjelmalla. Hallintaohjelma myös valvoo, ettei vanhoja salasanoja käytetä uudestaan. Salasanatietokanta säilötään palvelimella, jotta sitä voi käyttää kaikki työn-

tekijät samanaikaisesti ja samalla tietokanta pysyy varmuuskopioituna. Etätyöntekijätkin pystyvät käyttämään salasanatietokantaa VPN-yhteyden kautta.

Yritykseen myös hankitaan UPS-laite, joka on tarpeeksi tehokas tukemaan neljää pöytäkonetta ja suojaa sähkökatkoista johtuvaa tiedon menetystä tärkeimmistä laitteista. UPS-laite kytketään palvelimeen USB-johdolla, jotta UPS-laite saa sammuttaa palvelimen automaattisesti ja turvallisesti. Kaikkiin koneisiin myös tehdään automaattinen sammutus komentosarja, joka sulkee mahdolliset tärkeät ohjelmat ja sammuttaa koneen turvallisesti, jos tietokoneessa on käytössä patterivirta yli 30 sekunnin ajan yhtäjaksoisesti. Laite itsessään toimii jo jännitesuojana, joten ylimääräisten jännitesuojien hankkiminen ei ole tarpeellista.

Yrityksessä on myös palohälytin ja palosammutin, mutta ei automaattista sammutusjärjestelmää. Tulevaisuudessa yrityksen kannattaisi myös harkita, vaikka remonttien aikana, hankkivansa infrastruktuurin vikojen tunnistimia. Automaattisia veden sulkijoita ja automaattista sammutusjärjestelmää myös suositellaan hankkivan. Tunnistimet, sulkimet ja sammutusjärjestelmät suojaavat yritystä silloinkin kun yrityksen tiloissa ei ole ketään paikalla.

Käyttöjärjestelmien automaattiset päivitykset varmistetaan olevan käytössä ja niitä tulee yrityksessä käyttää. Sovellusten päivittäminen tulisi tehdä aina kun mahdollista, mutta vain tärkeät tietosuojapäivitykset tulisi tehdä työpäivän aikana. Sovellusten yleiset päivitykset voidaan tehdä iltapäivällä ennen työajan loppumista.

Yrityksen tilat ovat jo valmiiksi hyvin ilmastoituja ja ne pysyvät ympäri vuoden hyvissä olosuhteissa tietokoneille. Yrityksen tulee siivota tilojaan hyvin ja pitää tilansa siistinä vähentääkseen mahdollisia pölystä johtuvia laitteiden ylikuumenemisongelmia. Yrityksessä tulisi aina olla paineilmapurkki ja mikrokuituliinoja tietokoneiden sisällä olevien pölyjen puhdistamista varten. Tietokoneet tulisi siivota vähintään 6 kuukauden välein täydellisesti, jotta niiden toimivuus voidaan taata pitemmäksi ajaksi.

Yritys pyrkii käyttämään tietokoneitaan ja laitteitaan mahdollisimman pitkään, joten vanhoja laitteita aletaan korvata vasta noin viiden vuoden käytön jälkeen. Hajonneet

laitteet kuitenkin korvataan heti uusilla laitteilla. Varaosia yritykseen ei valmiiksi hankita, joten yhtäkkiset laiterikot tulevat vähentämään yrityksen työntekijöiden työtehoa. Näissä tapauksissa työntekijät voivat kuitenkin tehdä etätöitä, jos se on mahdollista.

Yrityksessä on jo tarpeeksi hyvät murtautumisen hälytysjärjestelmät. Yritykseen kuitenkin hankitaan valvontakamera. Se toimii hyvänä esteenä varkauksien tapahtumisille päivän aikana, kun yrityksen tiloissa liikkuu työntekijöitä ja asiakkaita. Kameran avulla voidaan saada myös selville työntekijöiden tekemiä huolimattomuudesta johtuvia virheitä. Valvontakamera auttaa myös saamaan mahdolliset murtautujat helpommin kiinni.

Kaikkien tehtävien muutosten yhteishinta pysyy suhteellisen matalana. Tällaisilla muutoksilla pystytään lisäämään yrityksen tietoturvaa huomattavasti. Yrityksen työntekijöiden työtunteja kuitenkin kuluu jonkin verran järjestelmien käyttämisen ja tietoturvallisemman käyttäytymisen opetteluun. Jatkossa myös työntekijät saattavat joutua käyttämään työaikaa järjestelmien ylläpitämiseen, hoitamiseen ja huoltamiseen.

LÄHTEET

AppliedTrust www sivut 2017. Every company needs to have a security program. Viitattu 16.6.2017. https://www.appliedtrust.com/resources/security/every-company-needs-to-have-a-security-program

Ascenzo, W. 2016. How RAID Fault Tolerance Works. Colocation America www-sivut. Viitattu 22.8.2017. https://www.colocationamerica.com/blog/what-is-raid-fault-tolerance

AVTECH www sivut 2016. An Updated Look at Recommended Data Center Temperature and Humidity. Viitattu 23.4.2017. https://avtech.com/articles/4957/updated-look-recommended-data-center-temperature-humidity/

Chiasson, S., van Oorschot, P, C. 2015. Quantifying the Security Advantage of Password Expiration Policies. Viitattu 12.8.2017. http://people.scs.carleton.ca/~paulv/papers/expiration-authorcopy.pdf

Chu, W. 2015. Which RAID Configuration Works Best for Your Business?. Newegg Business www-sivut. Viitattu 22.8.2017. https://blog.neweggbusiness.com/over-easy/raid-configuration-works-best-business/

Derek, M. 2014. This intelligent water leak detection system turns off your water if a pipe bursts. Treehugger www sivut. Viitattu 15.7.2017. https://www.treehugger.com/gadgets/water-hero-wireless-leak-detection-system.html

Deursen, N. 2015. How to reduce human error in information security incidents. SecurityIntelligence www-sivut. Viitattu 18.5.2017. https://securityintelligence.com/how-to-reduce-human-error-in-information-security-incidents/

Digital Preservation Management www sivut 2003. Physical Threats. Viitattu 16.4.2017. http://www.dpworkshop.org/dpm-eng/oldmedia/threats.html

Emma W. 2017. What does the NSCS think of password managers?. National Cyber Security Center www-sivut. Viitattu 15.9.2017. https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers

Hughes, J. 2017. The Best Firewall/Router for a Small Business. Manx Technology Group www-sivut. Viitattu 4.8.2017. https://www.mtg.im/the-best-firewall-router-for-a-small-business/

InfoSec Institute www-sivut. 2012. VLAN Network Segmentation and Security-Chapter 5. Viitattu 17.8.2017. http://resources.infosecinstitute.com/vlan-network-chapter-5/

Jacobi, J. L. 2016. Hard-core data preservation: The best media and methods for archiving your data. PCWorld www-sivut. Viitattu 13.9.2017. https://www.pcworld.com/article/2984597/storage/hard-core-data-preservation-the-best-media-and-methods-for-archiving-your-data.html

Kaspersky www-sivut 2017. Safety 101: Main sources of threats penetration. Viitattu 19.4.2017. https://support.kaspersky.com/viruses/general/789

Krzyzewski, J. 2014. The Importance of IT Policies. Protocol Policy Systems. Viitattu 25.6.2017. http://protocolpolicy.com/wp-content/uploads/2017/05/Policy-Whitepaper-The-Importance-of-IT-Policies.pdf

Leonard, P. 2016. 3 Places to Backup Your Company’s Data. My IT www-sivut. Viitattu 20.8.2017. https://www.myitsupport.com/blog/3-places-to-backup-your-companys-data

Like Geeks www-sivut. 2017. Hard Drive Encryption. Viitattu 20.8.2017. https://likegeeks.com/hard-drive-encryption/

Loiste www-sivut. 2017. Sähkökatkoihin varautuminen. Viitattu 14.9.2017. https://www.loiste.fi/sahkonsiirto/sahkon-laatu/sahkokatkoihin-varautuminen

May, A. 2017. Password expert says he was wrong: Numbers, capital letters and symbols are useless. USA Today www-sivut. Viitattu 12.8.2017. https://www.usatoday.com/story/news/nation-now/2017/08/09/password-expert-says-he-wrong-numbers-capital-letters-and-symbols-useless/552013001/

McAfee www-sivut 2017. Defending Against Malware and Trojan Horse Threats. Viitattu 29.5.2017. https://home.mcafee.com/advicecenter/?id=ad_spyware_damatht&ctst=1

Metivier, B. 2017. Network Segmentation: Considerations for Design. Sage Data Security www-sivut. Viitattu 16.8.2017. https://www.sagedatasecurity.com/blog/network-segmentation-considerations-for-design

Moramarco, S. 2017. Best Tips For Creating Strong Passwords. InfoSec Institute www-sivut. Viitattu 21.8.2017. http://resources.infosecinstitute.com/category/enterprise/securityawareness/best-tips-for-creating-strong-passwords/

Mouna, J., Latifa, B. A. R, Anis, B. A. 2014. Classification of security threats in information systems. Procedia Computer Science. Viitattu 19.4.2017. http://ac.els-cdn.com/S1877050914006528/1-s2.0-S1877050914006528-main.pdf?_tid=178a1432-24dd-11e7-a8cb-00000aab0f26&acdnat=1492591946_7560912f3544ffad442604b280342fd3

Munroe, R. 2011. Password Strength. xkcd www-sivut. Viitattu 17.8.2017. https://xkcd.com/936/

National Cyber Security Center www-sivut. 2016. Password Guidance: Simplifying Your Approach. Viitattu 12.8.2017. https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

Newman, R. 2010. Computer Security: Protecting Digital Resources. Viitattu 28.5.2017. https://books.google.fi/books?id=0QvNLy-j4uoC&printsec=frontcover

Nordquist, B. 2017. When Should You Replace Your Server. Storagecraft www sivut. Viitattu 15.5.2017. https://www.storagecraft.com/blog/when-should-you-replace-your-server/

Norton www-sivut 2016. Bots and Botnets – A Growing Threat. Viitattu 30.5.2017. https://us.norton.com/botnet/

PivotStor www-sivut. 2016. Why a tape backup system is still a good storage option. Viitattu 21.9.2017. http://pivotstor.com/lto-tape-news/tape-backup-system-still-good-storage-option/

Porin kaupungin www sivut. 2017. Tulvasuojelu taustaa. Viitattu 24.4.2017. https://www.pori.fi/tpk/tulvasuojelu/taustaa.html

Power Shield www-sivut. 2017. Benefits of Uninterruptable Power Source (UPS). Viitattu 19.4.2017. http://powershield.com.au/benefits-of-uninterruptible-power-supply-ups/

Richmond, R. 2012. How to Maintain Security When Employees Work Remotely. Entrepreneur www-sivut. Viitattu 19.8.2017. https://www.entrepreneur.com/article/224241

Rood, S. C. 1996. Computer Hardware Maintenance: An IS/IT Manager's Guide. Viitattu 15.5.2017. https://books.google.fi/books?id=qF2w2CsdGB0C&lpg=PA3&dq=computer%20hardware%20maintenance&pg=PP1#v=onepage&q&f=false

Rytmi Rakennus Oy www sivut. Kodin turvajärjestelmät. Viitattu 15.7.2017. http://www.rytmirakennus.fi/sisaremontit/sahkoremontti/kodin-turvajarjestelmat/

Sanchez, M. 2010. The 10 most common security threats explained. Cisco. Viitattu 19.4.2017. https://blogs.cisco.com/smallbusiness/the-10-most-common-security-threats-explained

SecuritySystemReviews www sivut 2014. Types of Security System Equipment. Viitattu 10.7.2017. http://www.securitysystemreviews.com/types-of-security-system-equipment/

Steers, K. 2004. Hardware Tips: Complete PC Preventive Maintenance Guide. PCWorld. Viitattu 15.5.2017. http://www.pcworld.com/article/116583/article.html

Stevens, P. S. 2016. The Best Antivirus Software for Business: Our Top Picks. Business News Daily www-sivut. Viitattu 10.8.2017. http://www.businessnewsdaily.com/2513-antivirus-software-business.html

StorageSwiss www-sivut. 2017. The Role of Tape in Today's Data Center. Viitattu 21.9.2017. https://storageswiss.com/2017/03/21/role-of-tape-in-todays-data-center/

Symantec 2015. Keeping Your Private Data Secure. Viitattu 17.9.2017. https://www.symantec.com/content/dam/symantec/docs/white-papers/keeping-your-private-data-secure-en.pdf

Taloushallintoliiton www-sivut. 2015. Kirjanpidon vaatimukset riippuvat yrityksen koosta. Viitattu 8.9.2017. https://taloushallintoliitto.fi/sv/node/427

TechAdvisory www-sivut. 2017. Firewalls: hardware vs. software. Viitattu 2.8.2017. http://www.techadvisory.org/2017/03/firewalls-hardware-vs-software/

The University of Edinburgh www-sivut. 2017. Choosing strong passwords. Viitattu 21.8.2017. http://www.ed.ac.uk/infosec/how-to-protect/lock-your-devices/passwords/choosing-strong-passwords

Ubiquiti Networks www-sivut. 2017. UniFi -Wireless Guest Network Setup. Viitattu 16.8.2017. https://help.ubnt.com/hc/en-us/articles/115000166827-UniFi-Wireless-Guest-Network-Setup

Wallace, C. 2015. How to Disaster-Proof Your Server Room. Newegg Business blog. Viitattu 24.4.2017. https://blog.neweggbusiness.com/over-easy/how-to-disaster-proof-your-server-room/

Yeagley, G. 2015. IT Security Policies and Procedures: Why You Need Them. Compass IT Compliance www-sivut. Viitattu 21.9.2017. https://www.compassitc.com/blog/it-security-policies-and-procedures-why-you-need-them

Yrittäjät www-sivut. 2017. Yrittäjyys Suomessa. Viitattu 8.9.2017. https://www.yrittajat.fi/suomen-yrittajat/yrittajyys-suomessa-316363

Zhang, Y., Monrose, F., Reiter, M, K. 2010. The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis. Viitattu 12.8.2017. https://www.cs.unc.edu/~reiter/papers/2010/CCS.pdf